A Privacy-Preserving and Vessel Authentication Scheme Using Automatic Identification System

Pengchuan Su
Beijing Institute of Technology
supc@bit.edu.cn

Nan Sun *
Beijing Institute of Technology
sunnan@bit.edu.cn

Liehuang Zhu
Beijing Institute of Technology
liehuangz@bit.edu.cn

Yandong Li
Beijing Institute of Technology
leeyandong@bit.edu.cn

Rongrong Bi
China National Software and Services Co. Ltd.
birr@css.com.cn

Meng Li
Beijing Institute of Technology
menglibit@bit.edu.cn

Zijian Zhang
Beijing Institute of Technology
zhangzijian@bit.edu.cn

ABSTRACT

Automatic Identification System (AIS) has been widely used in smart vessel transportation aiding collision avoidance, search, rescue and traffic monitoring nowadays. AIS transceiver adopts a unique Maritime Mobile Service Identity (MMSI) to identify a vessel uniquely. However, this identity is now simple to be forged and tampered. Besides, AIS transceiver broadcasts voyage information automatically and continuously, which makes it possible to be tracked when communicating with the sea-side infrastructures or other vessels. Thus, it poses a serious threat to vessel trajectory privacy. To tackle this problem, we first propose a Digital Certificate based Identity Authentication Scheme (IAS) to ensure the authenticity of the AIS data source. Secondly, we further propose a Mix-zone and Blind-signature based Trajectory Privacy Protection Scheme (TPPS) to guarantee that the vessel identity and trajectory information will not be leaked without losing AIS basic function. Finally we analyse the security of our scheme. The experimental results show that our scheme has the same magnitude order of time-consuming compared with the ordinary AIS data pack and unpack protocol.

Keywords

AIS, Authentication, Privacy-Preserving

1. INTRODUCTION

With the rapid commercial economic development, the maritime transportation becomes popular all over the world. At the same time, the growing number of vessels makes it urgent to improve the technology for ship communication and safety preserving. For facilitating the management of maritime traffic and guaranteeing the safety of life at sea, the Automatic Identification System(AIS) [10] used as a vessel traffic management system came into service in 2001. It works through acquiring GPS coordinates and exchanging up-to-date information via radio transmissions and the information includes latitude, longitude, speed, heading and so on. AIS is generally used by vessels to monitor the surrounding sea traffic to avoid the occurrence of vessel collisions. And when vessels in danger are remote from the base station, they can also get in touch with the AIS management center and send the position information to wait for further rescue. In addition, AIS also helps maritime authorities grasp the traffic conditions and provides a powerful data basis for discovering illegal or abnormal vessels. According to a popular provider, AIS is currently used in smart transportation widely with an estimated number of over 300,000 installations. And actually there are still many unregistered vessels all over the world, which makes the number of AIS-equipped vessels higher.

Given its increasing importance and prevalence in maritime traffic safety, we found there are still some security problems to be solved in AIS. MMSI in AIS data is a unique sequence of 9 digital numbers given to every vessel for AIS identity authentication. However, the authentication mechanism in current AIS data protocol is not perfect, making MMSI number easy to be fogged and tampered. According to analysis of the tremendous amount of real AIS data, we found that it is common for several vessels to share one MMSI number [13], which means that a vessel navigating with a certain MMSI number may not be the real one, causing the problem of identity theft. In fact, the crew may optionally enter MMSI number or use the default MMSI number when operating AIS equipment for some malicious purpose or carelessness [16], for example, smugglers may attempt to hide their information of nationality. Shared or forged MMSI will weaken the function of AIS, making illegal vessels forge shipping status to evade the law enforcement. Besides, it is difficult for maritime rescue departments to conduct ac-

*This author is the corresponding author.

SCC'17, April 02 2017, Abu Dhabi, United Arab Emirates

DOI: http://dx.doi.org/10.1145/3055259.3055261

curate rescue measures for vessels in danger according to the MMSI number.

Moreover, the working principle of AIS transceivers to broadcast vesselą́s voyage information automatically and periodically makes it possible to track a vessel based on its data transmissions with the sea-side infrastructure or other vessels. And nowadays AIS data can be collected easily by someone who has an AIS data receiver and there are also tradings from AIS data providers to other institutions in commercial forms. As the AIS data contains abundant spatial and temporal information, attackers can infer the private navigation trajectory information of vessels with a high probability by collecting trajectory data sets, which poses a serious threat to vessel trajectory privacy. For example, for some shipping companies, AIS data may contain valuable business information through which the competitors may find the merchant ships' main business areas, even the business models. In addition, the openness of trajectory data means that an arbitrary organization can obtain the navigation information about vessels and lead to illegal collection or transactions of information on vessels. And illegal organizations including pirates can also access the corresponding trajectory of merchant to loot, which is a huge threat to the merchant's life and property [4].

Although the above-mentioned problems have not caused widespread awareness of crisis to date, it is necessary and urgent to improve the way to authenticate vesselsą́ identity and protect their trajectory privacy. In this paper, a scheme of AIS data protocol supporting vessel identity authentication and trajectory privacy protection is proposed for the first time to the best of our knowledge, using the theory of digital certificate and k-pseudonym scheme to ensure that the vessel identity and voyage trajectory information will not be leaked without losing the basic function of AIS.

We summarize our contributions as following:

1. We find a loophole of AIS protocol and propose a Digital Certificate based AIS Authentication Scheme, which can authenticate the AIS data source and ensure that the identity of the AIS will not be forged or tampered.

2. We further combine Mix-zone and Blind-signature to propose a Trajectory Privacy Protection Scheme, in order to protect trajectory privacy without losing basic function of AIS.

3. We make a security analysis and conduct an performance evaluation of our scheme. The experimental results show that our scheme has the same magnitude order of time-consuming compared with the ordinary AIS data pack and unpack protocol.

The rest of the paper is recognized as follows. Section 2 overviews the related work. Section 3 recalls the preliminaries. In section 4, we describe the models and goals and then the detailed description of our scheme is presented in Section 5. Section 6 and section 7 provide the security analysis and performance evaluation respectively. And Section 8 concludes the paper finally.

2. RELATED WORK

AIS is now making a significant contribution to the efficiency of maritime traffic management, but there are also a variety of security threats. We briefly introduce the existing work about the AIS security and vessel trajectory privacy here.

2.1 AIS Security

There are several literatures focusing on correlating and analyzing AIS data or making various applications via AIS, like voyage safety, collision avoidance, navigation inspection, ease of oil waste and so on [3, 21, 20, 25]. But few has focused on the security problem of AIS data protocol. A security evaluation of AIS was conducted in [16] where Balduzzi et al. proved that there are several threats in both the protocol specification and implementation of AIS, by offering malicious action and attack possibilities using a software-based transmitter. Actually, the original purpose of AIS was mainly to guarantee the safety of nAbul:Neveravigation, and the security in current version is relatively weak given a number of critical shortcomings. In addition, there is no mechanism for identity authentication about the data sender or encryption processing for privacy information [16]. Problems may appear when researchers are trying to analyze the AIS data. As reported in [7], 52% of the messages in a sample data set had to be rejected as dirty data. As for the solutions towards these security problems, we found that the literature [2] proposed a detection method for errors, falsifications and undergo spoofing of AIS messages by studying the physical characteristics of the signal. And in literature [11], there is elaboration about security issues of satellite nodes exposure and open communication channel threats in the heterogeneous Internet environment.

2.2 Trajectory Privacy

Trajectory data has abundant temporal and spatial correlation information compared with simple location data, making attackers having an easier access to vessel privacy [15, 19]. A large number of schemes in trajectory privacy protection were based on K-anonymity methodology [1, 14, 9, 22, 17, 27, 23, 24]. The core idea of K-anonymity is summarizing k attribute values before publishing the record set, which is known as pseudonym corresponding to each record's identifier. Thus, it concealed the real identifier and made the k pseudonym public. Releasing anonymized trajectories may still have some privacy leaks, so in literature [22], a scheme was proposed by searching for some anonymized trajectories in a certain area with near space distance, because an area with more similar anonymized trajectories has an more effective result of privacy protection. To achieving the effect of anonymity, literature [26] took steps to make a trajectories division in both one-dimensional and two-dimensional space to obtain many track fragments instead of the full track information. Beresford et al. [5] firstly proposed a novel scheme based on the notion of Mix-zone for trajectory privacy protection, which has been well adopted in the literature [6, 12] as a measurement to improve the location privacy of mobile devices in road networks. The K-pseudonym scheme based on Mix-zone was also applied in the vehicle communication system based on ad-hoc network. The basic idea was to assign k pseudonyms to each vehicle as its public identities. When driving into a Mix-zone, it can change its public identity freely so that the disguised identities cannot be linked with each other. In that way, the vehicles trajectories will be concealed well. Although there are many researches aiming at trajectory privacy protection,

to the best of our knowledge, we are the first to adopt the Mix-zone theory into the field of AIS for vessels trajectory privacy.

3. PRELIMINARIES

3.1 Digital Signature

Digital signature based on asymmetric cryptography theory is an identity authentication mechanism which is a necessary condition of non-repudiation [8]. A signature scheme can be expressed as the triple $(KeyGen, Sign, Verify)$:

1. $KeyGen(1^k) \longrightarrow (p_k, s_k)$: $KeyGen$ is a key generation algorithm taking a security parameter k as input and a pair of keys (p_k, s_k) as outputs, where p_k is public, s_k is private and k is the least length of the keys.

2. $Sign(s_k, m) \longrightarrow \delta$: $Sign$ is a signing algorithm taking a private key s_k and message m as inputs and a signature δ as output.

3. $Verify(p_k, m, \delta) \longrightarrow v$: $Verify$ is a verification algorithm taking a public key p_k, a message m and a signature δ as inputs and two-value v as output. When $v = 1$, it means the signature is valid and $v = 0$ means the signature is not valid.

3.2 Public Key Certificate

The public key certificate [18] is also called digital signature. It is a document with content of identity information and key's ownership for users, computer systems and organizations. As a method for identity authentication, digital signature cannot make an identification of public key owner's identity. To ensure that the public key is owned by a certain entity, the corresponding relationship should be qualified by a trusted third party, which is called as Certification Authority(CA). In a typical public key infrastructure scheme, CA is a signer for usersąŕ identity and public key information and thus make a binding between the two. The binding relationship can be verified by the signature of CA.

3.3 Mix-zone

A Mix-zone is a region where k participants each has k pseudonyms and can change their pseudonyms freely so that the mapping between their old and new pseudonym will not be revealed. In a Mix-zone, a set of k participants enter in some order and none will leave before that are all in it. Inside the Mix-zone, the location information of the participants will not be reported and the leaving order is different with the beginning, in which way the relation between their entering and exiting events will be confused. A Mix-zone has the properties as follows. ***Definition 1***: A Mix-zone M can provide k-anonymity to a set of users U if and only if:

1. U has k or more than k members, i.e., $|U| > k$.

2. None of the k members will exit before they all enter M and there must be a time point when all the k members of U are in the zone.

3. For each $u \in U$, entering M at the time $i_u \in I$ and leaving M at time $o_u \in O$ will take a completely random time in the M.

4. The probability of transition between arbitrary $i \in I$ and arbitrary $o \in O$ is following a uniform distribution.

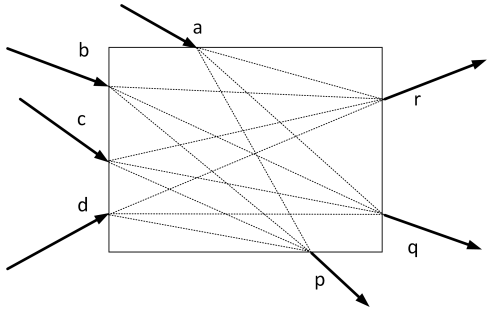

Figure 1: Mix-zone Model

An example of Mix-zone with three members is shown in *Figure 1*. The members enter in the zone using the pseudonyms a, b and c and exit the zone with the pseudonyms p,q and r. Given arbitrary pseudonym in $\{p, q, r\}$, the adversary has equal probability to find the pseudonym in $\{a, b, c\}$ corresponding with it, in other words, the Mix-zone provides an anonymity of $K = 3$.

3.4 Blind Signature

The blind signature is a form of digital signature in which the content of the message is disguised before signed. One of the simplest of blind signature is based on RSA signing. Assume that the PK is (d, n) while the SK is (e, n). And there are three parts of the signature.

1. $Sign(SK, Digest(m) \times r) \longrightarrow \delta$: A user computes the digest of the content m and chooses a random number r to mix the message. And the CA uses the SK to sign the message as $(Digest(m) \times r)^e \ mod \ n$.

2. $Save(PK, \delta, r) \longrightarrow \delta^{'}$: After getting the signature, the user will remove r like $\delta^{'} (\leftarrow \delta \times r^d)/r \ mod \ n$.

3. $Verify(PK, m, \delta^{'}) \longrightarrow v$: Using the PK to verify the signature like $Digest(m) \stackrel{?}{\equiv} \delta^{'d} \ mod \ n$. If the equation is satisfied, it means the signature is valid and $v = 1$ while $v = 0$ means the signature is not valid.

4. MODELS AND GOALS

4.1 System Model

In this paper, our system model as shown in *Figure2* has three different entities including ship, shore-based station and AIS center.There is ship-borne equipment installed in ship which is a communication process unit. For every equipment, before accessing to the network, there must be a registration in authority to apply for its common arguments, and private key which will be stored in ship devices with tampering prevention and authorized access. The shore-based station is kind of infrastructure deployed along the coast and is a gateway in the communication network. AIS center has two roles: service provider(SP) and trusted authority(TA) respectively. SP provides some functional service. For example, search and rescue positioning. TA is a trusted security center and registration authority of the whole system, bearing the responsibility including the registration of base stations and ship-borne devices. The system has three communication modes: through the frequency channel of

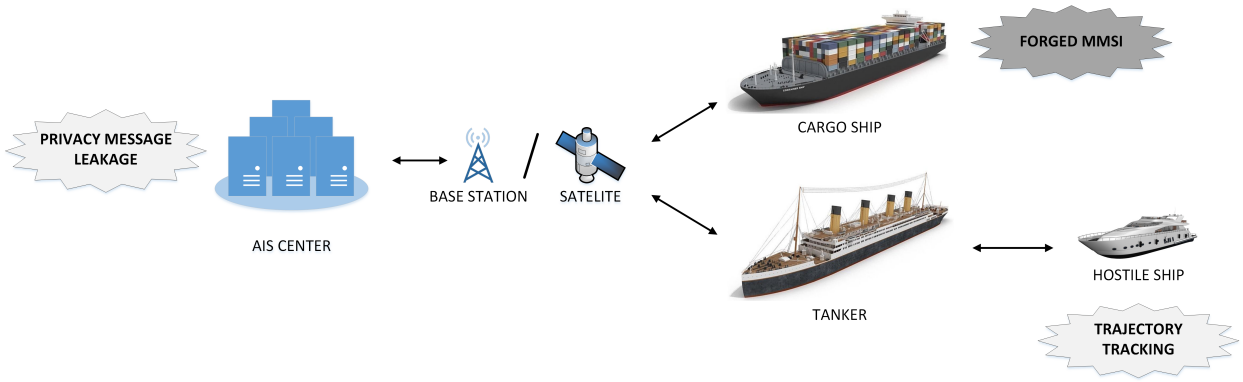

Figure 2: AIS System and Attack Model

VHF, satellite communication and private communication with vessel traffic system. VHF is the most frequently used mode with a limited transmission distance of 20 to 30 nautical miles bounded by the VHF frequency characteristic. AIS equipments can communicate with others or shore stations through the VHF channel. In the regions with no base station built, the satellite communication can be used. When vessels are entering in the customs management regions, they can access to the custom network and make a private communication in a secure channel.

4.2 Adversary Model

In our adversary model as shown in *Figure2*, Assume that there are internal and external attackers. Vessel itself is considered as an internal attacker in the way of forging the identity information of itself or personating other vessel to send false information. The honest but curious AIS center may also play a role of internal attacker by collecting the vesselsą́ trajectory information. As for some organizations attempting to obtain other vessels' identity or trajectory information, we think that they are external attackers, including other vessels, base station and so on. When vessels are in the communication mode of VHF, we assume that a passive adversary who has perfect eavesdropping ability can obtain all the voyage information of a vessel in the effective communication range.

4.3 Design Goals

In this paper, we expand the original data protocol of AIS system in the following three goals:

Functional Goal: Our scheme works on expanding the fundamental scheme of AIS system while holding its inherent functions. The expanded scheme guarantees that vessels can still exchange information with other vessels in a certain range.

Security Goal: Our scheme is with the security property of authentication, non-repudiation and traceability. Authentication is about the confirmation on entity and message integrity, which help to verify the authenticity of message sendersą́ identity information and ensuring that the message is not tampered during the transmission process. Non-repudiation is about the property that the vessel cannot deny the fact of having sent any messages. And traceability is to ensure that AIS center can make a certification on vessels identity.

Privacy Goal: Our scheme protect vessels identity privacy and trajectory privacy. For a general messages receiver, like a vessel, it can verify the authenticity and integrity of the senderą́s identity information while cannot learn which vessel it is exactly. Meanwhile, it is difficult for a general messages receiver to track other vesselsą́ trajectory.

5. SCHEME

Our scheme consists of two parts, one is for message source authentication, and the other is trajectory privacy preserving. Firstly, we introduce digital certificate into the AIS data protocol to guarantee the authenticity of AIS data source and ensure that the identity field cannot be tampered and forged. Then we propose a scheme based on Mix-zone theory to protect vessels' identity and trajectory privacy.

5.1 Digital Certificate based Identity Authentication Scheme

In this section, vessel can verify message senders' identity through the three communication modes above-mentioned. We assume that Vessel A is the message sender, Vessel B is the message receiver, and the shore station H is participating the communication among them. The message is divided into four parts, including certificate, data information such as location and speed, time stamp and the digital signature of message sender. There are three parts in our scheme as shown in *Figure3*.

5.1.1 Setup

For a AIS ship-borne device of a vessel which ready to put into use. Such as vessel A, there should be a pair of public and private key PK_A, SK_A generated by its owner ship for it and then the owner ship should submit the identity information and public key PK_A to the official trusted institution, which in our scheme is the AIS center. The following job of AIS center is to generate a certificate $Cert_A$ for vessel A using the private key SK_{CA} of itself and store it in vessel A's AIS device. The content of $Cert_A$, shown in *Equation 3*, includes the name of certificate issuing agency $Name_{CA}$, the MMSI code $MMSI_A$, the valid date of the certificate $ValidDate$, certificate owner's public key PK_A and Sig_{cert} shown in *Equation 2*, which is the signature of the above information using the private key of CA. *Digest* is a digest algorithm. The important role of the certificate is an official authentication for vessels' MMSI field.

$$Info_{cert} = Name_{CA}||MMSI_A||ValidDate||PK_A \quad (1)$$

$$Sig_{cert} = Sign(Digest(Info_{cert}), SK_{CA}) \quad (2)$$

Algorithm 1 Verification

Input:M

Output: v

1: $v = 0$
2: $M = (Cert_A, T, Data_{dyna}, Sig_A)$
3: $Cert_A = (Name_{CA}, MMSI_A, ValidDate, PK_A, Sig_{cert})$
4: **if** $ValidDate$ is valid **and** $Verify(PK_{CA}, Sig_{cert})$ **then**
5: $\quad v = Verify(PK_A, Sig_A)$
6: **else**
7: $\quad v = 0$
8: **return** result

$$Cert_A = Info_{cert}||Sig_{cert} \tag{3}$$

5.1.2 Sign and Send Data

The next step is to sign for AIS data with A's private key. Considering the way of data transmission, time stamp T is the data to be signed to prevent the replay attack. Finally the AIS data format M is shown in *Equation 6*.

$$Data_{dyna} = ROT||COG||SOG||LNG||LAT||HEADING \tag{4}$$

$$Sig_A = Sign(T, PK_A) \tag{5}$$

$$M = Cert_A||T||Data_{dyna}||Sig_A \tag{6}$$

5.1.3 Verify Data

The verification work is done by the message receiver B according to the procedure shown in *Algorithm 1*. The input is the message M and the output v is a two-value variable. When $v = 1$ it means that the data is from vessel whose MMSI code is $MMSI_A$ without replay attack, while $v = 0$ means that M cannot be verified. The algorithm is implemented in the following steps. Firstly the several parts of M and $Cert_A$ will be separated. If $ValidDate$ is in valid time range and Sig_{cert} is verified, the next step should be a verification about Sig_A using PK_A to make sure that the message cannot be forged.

5.2 Mix-Zone based Trajectory Privacy Protection Scheme

The issue of vessel identity authentication is solved in the above scheme for the convenient of traffic management, however, there is another security demand of vessel identity and trajectory privacy in our scheme from the perspective of vessels. In this part of our scheme, the communication mode of VHF is discussed only for the purpose of privacy protection. There are three parts in our scheme.

5.2.1 Setup

Firstly the pseudonym is introduced to mark vessels' identity in the way of distributing K substitutes corresponding to the actual MMSI code for every vessels as the identity used to communicate with others, described as $\{S_1, S_2, ..., S_K\}$. The information of mapping relation will be stored in the AIS center only and other vessels have no way of distinguishing a vessel identity with the help of pseudonym. There are certificates one-to-one matching with each substitute of MMSI code. A special pseudonym may be wanted, which

Algorithm 2 Pseudonym Variation

Input: $P_A, \{S_1, S_2, ..., S_K\}, R, N, \{M_1, M_2, ..., M_H\}, S_p$

Output: S

1: $sum = 0, i = 0$
2: **while** $i <= H$ **do** ąąąą
3: $\quad$ Get the Position coordinate in $M_i : P_i$ ąąąą
4: $\quad$ Compute the distance d_i from P_A to P_i
5: $\quad$ **if** $d_i <= R$ **then**
6: $\quad\quad sum++$
7: $\quad i++$
8: **if** $sum >= n$ **then**
9: $\quad S = S_k$, where k is chosen randomly
10: **else**
11: $\quad S = S_p$
12: **return** S

can be used when vessels run into a danger to reduce computational complexity for AIS center, thus to provide a timely aid for the vessel in the rescue requirement. The $Sig_{cert_i}$and $Cert_{A_i}$are shown in formula *Equation 8* and *Equation 9*.

$$Info_{cert_i} = Name_{CA}||S_i||ValidDate||PK_A \tag{7}$$

$$Sig_{cert_i} = Sign(Digest(Info_{cert_i}), SK_{CA}) \tag{8}$$

$$Cert_{A_i} = Info_{cert_i}||Sig_{cert_i} \tag{9}$$

5.2.2 Sign and Send Data

To hiding the information of trajectory, vessels will change the pseudonym and certificate in AIS data constantly with a certain frequency. Before sending the AIS data, vessel A will compute the vessels number n in the area within its effective communication distance R according to the last AIS messages $\{M_1, M_2, ..., M_H\}$ it received. It is the time to change the pseudonym and certificate if n is up to the threshold N, when a Mix-zone is formed, by selecting one randomly in the $K-1$ substitutes. Obviously, the navigation information of vessel A is secret for vessels out of the effective communication area. And for vessels within the area, the pseudonym changing scheme can make it difficult to link two pseudonyms, one of which is used before entering into the Mix-zone and the other is used when vessel A have exited from the Mix-zone, thus to prevent attackers from analysing the trajectory information of vessel A from the regularity of pseudonym changing. The position coordinate of vessel A is P_A. S_p is the pseudonym used on the present moment. The algorithm is shown in *Algorithm 2*.

5.2.3 Verify

The work of verification is the same as the first scheme. Although the identity code is a pseudonym, it can still be proved if the AIS message is valid because of the certificate of pseudonym.

5.3 Blind-Signature based Trajectory Privacy Protection Scheme

The trajectory privacy protection is solved among vessels, but the CA knows the relationship of every pseudonym

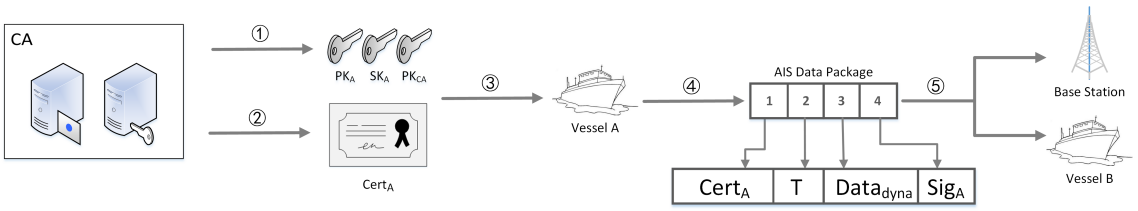

Figure 3: System Model

to the real identity. To solve this problem, we use blind-signature to sign the pseudonym which is provided by the vessel. There are three parts in our scheme.

5.3.1 Setup

To hiding the relationship between pseudonym and real identity, the selection of pseudonym must be executed by the vessel. The vessel generates K pseudonyms like $\{S_1, S_2, ..., S_K\}$. And then, the vessel send the $Digest(S_i) \times r$ to CA, while r is a random number. The CA signs the message and gives a feedback to the vessel. The Sig_{Cert_i} is shown in formula *Equation 11*. The vessel need to removes the number r after receives the feedback, and gets the $Cert_{Ai}$ like the formula *Equation 12*.

$$Info_{Digest} = Digest(Name_{CA}) \times Digest(S_i) \times Digest(ValidData) \times Digest(PK_A) \times r \quad (10)$$

$$Sig_{cert_i} = (Info_{Digest})^{SK_{CA}} \quad (11)$$

$$Cert_{A_i} = (Info_{cert_i} || Sig_{cert_i} \times r^{PK_{CA}})/r \quad (12)$$

5.3.2 Sign and Send Data

The work of this part is the same as the second scheme. Although the signature of the certification is different from the second scheme.

5.3.3 Verify

After B receives the message from A, it will verify the validity of the message. The verification work may be different from the first scheme, because the way of signature is changed. At first, B should get the digest of each part of the $Info_{cert_i}$. And then, B will judge the satisfaction of the formula *Equation 13*. If it is, B will verify Sig_a by using PK_A.

$$Cert_{A_i}^{PK_{CA}} \stackrel{?}{=} Digest(Name_{CA}) \times Digest(S_i) \times Digest(ValidData) \times Digest(PK_A) \quad (13)$$

6. SECURITY ANALYSIS

In this session, we analyze the security of our scheme from the aspects of non-repudiation, anonymous authentication and non-connectability.

Non-Repudiation: In our scheme, digital certificate ensures that the certificate of one entity can be generated only by itself because the essential characteristic of digital certificate is to generate a certificate with the signer's private key. When there is a disputation about message's sender, CA can make a judgement according to the certificate.

Anonymous Authentication: In our scheme, vessels communicate with others using their pseudonyms and there are legal certificates for every pseudonyms. So the anonymous authentication can be ensured.

Non-Connectability: In our scheme, vessels cannot learn the true identity information of a message sender. So even if a vessel receives different messages of one vessel, it cannot prove that the messages are from one vessel.

Table 1: Configuration Parameters

Item	Parameter
`Operation system`	Windows 10(64bit)
`CPU Version`	Intel(R) Core(TM) i5-4590
`Memory`	4GB

Table 2: Programming Reference

Item	Reference
`Coding Language`	Java
`Cryptography Library`	Bouncy Castle
`Communication Protocol`	UDP

7. PERFORMANCE EVALUATION

In this session, we conduct a performance evaluation of our scheme compared with the ordinary AIS data protocol. The communication equipment is two personal computers and one is AIS data sender, the other is receiver. The experimental parameters is shown in *Table 1* and *Table 2*. The operation system is Windows 10(64bits) and with the 4GB memory. The CPU version is Intel(R) Core(TM) i5-4590. The program is coded with Java language. Since the scheme is implemented in the ship-borne device and is irrelevant with the communication mode, we simulate the AIS communication protocol using UDP protocol. The cryptography algorithms are realized by calling the Bouncy Castle Library. The program is based on the real AIS data format and is run for 300 times. Finally the result is the mean of 300 time-consuming value. The result in *Figure 4* shows that our scheme has the same magnitude order of time-consuming compared with the ordinary AIS data pack and unpack protocol.

8. CONCLUSIONS

AIS is a cyber-physical system commonly used in the marine industry for vessels traffic monitoring and assistance. In this paper, the security issues about vessel identity authentication and trajectory privacy protection are discussed based on the conventional application scenarios of AIS in maritime traffic. Moreover, a data protocol supporting the identity authentication and trajectory privacy protection is

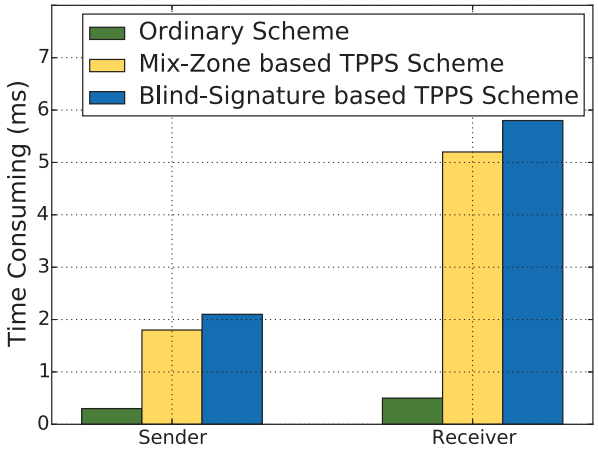

Figure 4: Experimental Result

proposed based on the theory of public key certificate and Mix-zone. Finally, the security attributes of our schemes are analysed and the performance evaluation is conducted, which proves that the scheme has a good performance of security and effectiveness.

9. ACKNOWLEDGMENTS

This work is partially supported by China National Key Research and Development Program No. 2016YFB0800301.

10. REFERENCES

[1] O. Abul, F. Bonchi, and M. Nanni. Never walk alone: Uncertainty for anonymity in moving objects databases. In *IEEE International Conference on Data Engineering*, pages 376–385, 2008.

[2] E. Alincourt, C. Ray, P. M. Ricordel, D. Dare-Emzivat, and A. Boudraa. Methodology for ais signature identification through magnitude and temporal characterization. In *Oceans*, pages 1–6, 2016.

[3] C. Ambjorn. Seatrack web forecasts and backtracking of oil spills - an efficient tool to find illegal spills using ais. In *US/EU-Baltic International Symposium, 2008 IEEE/OES*, pages 1–9, 2008.

[4] M. Balduzzi, A. Pasta, and K. Wilhoit. A security evaluation of ais automated identification system. In *The Computer Security Applications Conference*, pages 436–445, 2014.

[5] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *Pervasive Computing IEEE*, 2(1):46–55, 2003.

[6] L. Buttyĺćn, T. Holczer, and I. Vajda. On the effectiveness of changing pseudonyms to provide location privacy in vanets. In *Security and Privacy in Ad-Hoc and Sensor Networks, European Workshop, Esas 2007, Cambridge, Uk, July 2-3, 2007, Proceedings*.

[7] B. R. Calder and K. Schwehr. Traffic analysis for the calibration of risk assessment methods. *Pediatric Nephrology*, 24(8):1453–1464, 2009.

[8] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[9] J. Domingo-Ferrer and R. Trujillo-Rasua. Microaggregation- and permutation-based anonymization of movement data. *Information Sciences*, 208(21):55–80, 2012.

[10] T. Eriksen, G. Høye, B. Narheim, and B. J. Meland. Maritime traffic monitoring using a space-based ais receiver. *Acta Astronautica*, 58(10):537–549, 2006.

[11] L. Fenghua, Y. Lihua, W. Wei, Z. Linjie, and S. Zhenguo. Research status and development trends of security assurance for space-ground integration information network. *Journal on Communications*, 37(11):156–168, 2016.

[12] J. Freudiger, M. Raya, M. Fĺęlegyhĺćzi, P. Papadimitratos, and J. P. Hubaux. Mix-zones for location privacy in vehicular networks. *In WiN-ITS 07*, 2007.

[13] Z. Gan and M. Song. Analyzing the problems in the implementation of mmsi. *China Maritime Safety*, 2009.

[14] S. Gao, J. Ma, C. Sun, and X. Li. Balancing trajectory privacy and data utility using a personalized anonymization model. *Journal of Network & Computer Applications*, 38(1):125–134, 2014.

[15] F. Giannotti, M. Nanni, F. Pinelli, and D. Pedreschi. Trajectory pattern mining. In *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 330–339, 2007.

[16] A. Haratimokhtari, A. Wall, and P. B. J. Wang. Automatic identification system (ais): Data reliability and human error implications. *Journal of Navigation*, 60(3):373–389, 2007.

[17] Z. Huo, Y. Huang, and X. Meng. History trajectory privacy-preserving through graph partition. In *International Workshop on Mobile Location-Based Service*, pages 71–78, 2011.

[18] J. W. G. Iii and K. F. E. Ip. *Protocols for Issuing public-key certificates over the Internet*. Springer Berlin Heidelberg, 1997.

[19] J. G. Lee, J. Han, X. Li, and H. Gonzalez. Traclass : trajectory classification using hierarchical region-based and trajectory-based clustering.

[20] L. I. Li-Na. Determination of the factors about safe distance of approach and etc on the research of ship automatic avoidance collision. *Journal of Dalian Maritime University*, 28(3):23–26, 2002.

[21] L. I. Li-Na, S. H. Yang, B. G. Cao, and L. I. Zi-Fu. A summary of studies on the automation of ship collision avoidance intelligence. *Journal of Jimei University*, 2006.

[22] M. E. Nergiz, M. Atzori, and Y. Saygin. Towards trajectory anonymization: a generalization-based approach. In *Sigspatial ACM Gis 2008 International Workshop on Security and Privacy in Gis and Lbs, Springl 2008, November 4, 2008, Irvine, California, Usa, Proceedings*, pages 52–61, 2008.

[23] P. Samarati. Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge & Data Engineering*, 13(6):1010–1027, 2001.

[24] P. Samarati and L. Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. 1998.

[25] K. D. Schwehr and P. A. Mcgillivary. Marine ship automatic identification system (ais) for enhanced coastal security capabilities: An oil spill tracking application. In *Oceans*, pages 1–9, 2007.

[26] H. Shin, J. Vaidya, V. Atluri, and S. Choi. Ensuring privacy and security for lbs through trajectory partitioning. In *Eleventh International Conference on Mobile Data Management*, pages 224–226, 2010.

[27] L. SWEENEY. k-anonymity: A model for protecting privacy. *IEEE Security & Privacy Magazine*, 10(5):1–14, 2012.